WHAT IS CLAIMED IS:

1   1.   A method for updating a program in a data processing system comprising the

2   steps of:

3   requesting a trusted platform module ("TPM") to perform a signature verification

4   of an update to the program;

5   the TPM performing the signature verification of the update to the program;

6   if the signature verification of the update to the program is successful, unlocking

7   a memory unit storing the program; and

8   modifying the program with the update to the program in response to the

9   unlocking of the memory unit storing the program.

1   2.   The method as recited in claim 1, further comprising the step of:

2   locking the memory unit after the modifying step.

1   3.   The method as recited in claim 2, wherein the locking step is performed by the

2   TPM.

1   4.   A computer program product adaptable for storage on a computer readable

2   medium and operable for updating a BIOS stored in a flash memory in a data processing

3   system, comprising:

4   a BIOS update application program receiving an updated BIOS image;

5   the BIOS update application requesting a TPM to perform a signature verification

6   of the updated BIOS image;

7   a TPM program receiving the request from the BIOS update application to

8   perform the signature verification of the updated BIOS image; and

9   the TPM program performing the signature verification of the updated BIOS

10   image and posting a result of the signature verification of the updated BIOS image to the

11   BIOS update application.

1   5.   The computer program product as recited in claim 4, further comprising:

2   if the result of the signature verification of the updated BIOS image determines

3   that the updated BIOS image is authentic, then the TPM program unlocks the flash

4   memory; and

5   the BIOS update application modifies the BIOS with the updated BIOS image.

1   6.   The computer program product as recited in claim 5, further comprising:

2   programming for locking the flash memory after the BIOS update application

3   modifies the BIOS with the updated BIOS image.

1   7.   The computer program product as recited in claim 6, further comprising:

2   if the result of the signature verification of the updated BIOS image determines

3   that the updated BIOS image is not authentic, then an error message is output.

1   8.   A data processing system having circuitry for updating a BIOS stored in a flash

2   memory in the data processing system, comprising:

3   input circuitry for receiving an updated BIOS image;

4   circuitry for requesting a TPM to perform a signature verification of the updated

5   BIOS image;

6   the TPM performing the signature verification of the updated BIOS image;

7   the TPM unlocking the flash memory if the signature verification of the updated

8   BIOS image determines that the updated BIOS image is authentic; and

9   circuitry for modifying the BIOS with the updated BIOS image.

1   9.   The system as recited in claim 8, further comprising:

2   circuitry for locking the flash memory after the BIOS is modified with the

3   updated BIOS image.

1   10.   The system as recited in claim 8, further comprising:

2   circuitry for outputting an error if the signature verification of the updated BIOS

3   image determines that the updated BIOS image is not authentic.